2012-02-22

CANADIAN SECURITY INTELLIGENCE SERVICE (CSIS)
INJURY ASSESSMENT REPORT PROVIDED FOR RCMP PROJECT STOIQUE

At this time, CSIS (the Service) can only provide preliminary findings and an initial assessment of the damage inflicted by the actions of Jeffrey Paul DELISLE. The full scope and nature of the injury, if ever fully known, can only be determined once the Service and its partners (domestic and foreign) have additional insight regarding DELISLE's access during the period in which he was providing information to the Russians, as well as the volume and specific documents he provided.

In his National Defence (ND) role, DELISLE had access to a secure Government of Canada (GoC) Top Secret network which contains highly classified documents. These include intelligence reports and assessments from several Canadian departments, including CSIS. Further, in October 2011, DELISLE commenced contact with the CSIS Atlantic Region office in his role as a Threat Assessment Officer at Trinity.

In addition to this access, DELISLE would have been in a position to provide the Russians with character assessments of individuals he had met within the Government of Canada (GoC), including at CSIS.

CSIS AND ITS MANDATE

In 1984, following the findings of the McDonald Commission, Parliament enacted the *Canadian Security Intelligence Service Act (CSIS Act)*. Pursuant to the *CSIS Act*, the mandate of the Service is to collect information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and reporting those threats to the GoC. The key areas investigated by the Service include: 1- Espionage or sabotage; 2- Foreign influenced activities within or related to Canada; 3- Activities within or related to Canada directed toward or in support of the threat of serious violence for the purpose of achieving political, religious or ideological objectives (i.e. terrorism); and 4- Activities directed toward undermining the constitutionally established system of government in Canada.

CSIS intelligence is shared with other federal departments and agencies, including the Department of Foreign Affairs and International Trade, Citizenship and Immigration Canada, the Canada Border Services Agency, National Defence, and the RCMP. The Service also has arrangements to provide security assessments to other countries and to share intelligence with other countries, as deemed appropriate.

The *CSIS Act* prohibits disclosures of information obtained by the Service in the course of its investigations, except in the performance of its duties and functions under the *Act*, or the

administration or enforcement of the *Act* or other laws. Section 19 of the *Act* also identifies other specific situations where such sharing of information is permitted:

- disclosures to law enforcement and to provincial or federal Attorneys General in an investigation or prosecution;
- disclosures to the Minister of National Defence or of Foreign Affairs, or departmental officials, when the information is relevant to matters relating to Canada's defence or international affairs; or
- disclosures authorized by the Minister of Public Safety that are considered to be in the public interest.

COOPERATION WITH FOREIGN AGENCIES

Cooperation with foreign agencies is vital to the Service's ability to advise the GoC on issues related to terrorism and other threats to the security of Canada. Chief amongst those agencies is an alliance known as the Five Eyes community, which is an intelligence sharing alliance composed of Australia, Canada, New Zealand, the United Kingdom and the United States.

Trust and confidence in the ability of a security intelligence agency, such as CSIS, to protect information are essential to the relationship which it has with the various foreign agencies that have entered into arrangements contemplated by section 17 of the *CSIS Act*. These relationships put the Service in a unique position of access to information that might otherwise be unavailable to Canada's intelligence community. Further, the Service does not have a foreign infrastructure to collect information to the extent of some of its partners. The Service continues to rely on foreign agency reporting in some circumstances to keep abreast of security threats and their development.

The sensitive information shared between various partners is invariably provided in confidence and on the express and / or implicit understanding that neither the information nor its source will be disclosed without the prior consent of the agency that provided it. Information is provided not only because of agreements to treat such information as classified, but because there is a confidence that the Service in particular, and the Canadian government in general, appreciate and acknowledge the need for confidentiality and has in place practices and procedures designed to safeguard such information.

If allied foreign agencies were to lose faith in the commitment of the Service or the GoC to protect such confidential information, there would be a significant detrimental impact on the willingness of other agencies to provide such information to the Service. Any reduction in the flow of information from foreign partners to Canada or diminution in its quality would serve to decrease the flow of information necessary to ensure the safety and protection of Canadians and Canadian interests.

DATE AND CIRCUMSTANCE OF THE BREACH

A breach of security occurs when any classified or designated information or asset is the subject of unauthorized access or disclosure. This may include unauthorized disclosure by any person, or theft, loss or exposure in circumstances that make it probable that unauthorized access or disclosure has occurred.

In a post arrest RCMP interview of DELISLE which took place on January 13, 2012, DELISLE admitted that in 2007 he walked into the Russian Embassy and from then on transmitted information from databases accessed at his work-site to the Russians for compensation. He normally received compensation by the Russians on a monthly basis, beginning in 2007. The Russians were looking for "anything related to their business" and specifically information on "western agents in Russia". According to DELISLE, the Russians sought to have him fill their intelligence gaps, which included "foreign agents" and the "energy sector" – specifically related to China and GoC relations. DELISLE stated he was asked to provide information from "Wiretaps basically or human gathering access".

On January 11, 2012, while operating under the belief he was communicating with the Russians, DELISLE passed classified documents, including two (2) CSIS Intelligence Reports (CIRs). These documents were classified "SECRET (CEO)" and "SECRET". Classified information is information that could reasonably be expected to cause injury to the national interest if compromised. Regarding the SECRET level, compromise could reasonably be expected to cause serious injury to the national interest. The Policy on Government Security defines the national interest as the security and the social, political and economic stability of Canada. The Service uses caveats in conjunction with a level of classification. Within the Service, the Canadian Eyes Only (CEO) caveat identifies classified information that cannot be shared with allied agencies.

The versions of the CIRs DELISLE attempted to share with the Russians on January 11, 2012 are identical to those CIRs disseminated by the Service to Canadian Government departments, including ND.

DESCRIPTION OF THE INFORMATION OR OTHER ASSETS CONCERNED INCLUDING THEIR SECURITY CLASSIFICATION AND SENSITIVITY

DELISLE attempted on January 11, 2012 to breach the entire contents of the following two CSIS documents:

1) CSIS Intelligence Report #1:
Classification: SECRET (CEO)
Dated: December 09, 2011
Dissemination: Ten (10) GoC departments, including National Defence (ND)
Synopsis: Russia-related
Extent of Potential Injury: HIGH

2) CSIS Intelligence Report #2:
Classification: SECRET
Dated: January 10, 2012
Dissemination: Four (4) GoC departments, including ND; and seven (7) foreign partners.
Synopsis: Russia-related
Extent of Potential Injury: HIGH

The unauthorized disclosure of information which could identify a Service source could cause exceptionally grave injury to the national interest. Based on the Service's analysis of the information contained in the two CSIS CIRs, the unauthorized release of these reports to a hostile foreign intelligence service could have allowed this foreign intelligence service to identify CSIS sources. As such, the extent of potential injury has been deemed to be 'HIGH'.

Both of the above CIRs contained explicit caveats which identify the reports as being the property of CSIS and that they may constitute "special operational information" as defined in *the Security of Information Act (SOIA)*. It is also noted in the caveats that the document must not be reclassified or disseminated, in whole or in part, without the consent of the Service. The full caveats are provided in the attached appendix. The *SOIA* defines special operational information as information that the GoC is taking measures to safeguard that reveals, for example: the identity of a confidential source of information; the means the GoC uses to covertly collect, or obtain or to assess, analyze, process, handle, report communicate or otherwise deal with information or intelligence; and whether a group, body or entity is the object of a covert investigation, or a covert collection of information or intelligence, by the GoC.

DELISLE was not / not authorized by the Service to disseminate this information, specifically to a foreign government for its benefit and, in so doing, acted contrary to the directions contained within these caveats.

DELISLE had access to a secure GoC Top Secret network which contains highly classified documents. It is noted that a high volume of CSIS documents are posted to this network and that DELISLE accessed the foregoing CIRs through this network. According to RCMP information stemming from the January 13, 2012 interview, DELISLE noted that (he) had passed "a lot" of information between 2007 and 2012, with information dumps effected electronically, occurring approximately the 10th of each month - everything was to be "fresh", as "old information is really not good information". Although DELISLE indicated that the information sent "wasn't a risk to our security", this is in contrast to his statement that "a lot of it was SIGINT" and that "some of it was CSIS reporting. I think it was a CSIS report. I sent some of those, but those are usually CEO DEFAIT (sic) related". He also noted that the most recent package, which he believed was sent circa January 10, 2012, was the "smallest package" that he had sent. The previous package was sent in "early December, maybe late November". He also had sent "contact lists" and "phone lists" of intelligence-related individuals in Canada and in the United States, in addition to other information from the United States, the United Kingdom and Australia.

ANALYSIS OF THE ACTUAL OR POTENTIAL INJURY TO NATIONAL INTERESTS THAT HAS RESULTED

This Injury Assessment addresses the actual or potential injury to national interests as a result of the attempted breach of the two CSIS reports described above.

The Service assesses that, had DELISLE successfully passed the two aforementioned CSIS reports to the Russians, the potential injury to the national interest would have been HIGH. Most detrimental to the Service and Canada was the potential for compromise of Service sources and the identity of a Service employee.

The Service assesses the following national interest and sensitive information would have been compromised as a result of this breach:

CIR #1 dated December 09, 2011: contains information relating to Investigations Pertaining to the Security of Canada, International Affairs and Defence, Economic Interests of Canada, and Personal Information.

CIR #2 dated January 10, 2012: contains information relating to International Affairs and Defence and Personal Information.

Of note, CIR #1 referred to previous Service reporting, with eight (8) specific CIR numbers. This could have provided the Russians with a "shopping list" of additional reports.

CSIS reporting, including the above and other CIR information, provided to ND between 2007 and 2012 emanates from Service sensitive sources. There is no doubt that some of this highly classified information, based on DELISLE's admissions, was provided to the Russians and, therefore, would have enabled them to fill Russian intelligence gaps to the detriment of Canada.

The Service does not disclose information, except as per section 19 of the CSIS Act, that would identify or tend to identify the Service's interest in individuals, groups or issues, including past or present files or investigations, the intensity of those investigations, or the degree or lack of success of investigations.

A security agency cannot operate effectively if the subjects of its investigations or other parties, such as a hostile agency, are able to ascertain the state of the security agency's operational knowledge at a particular point in time, the specific operational assessment made by the agency, or the fact that the agency is in a position to draw conclusions on a subject. Efficacy is also compromised if the subject of investigation or other unauthorized parties are able to ascertain what is already known about them, the methods of operation being used against them or the extent of coverage they are being afforded at various points in time. The disclosure of this information may put the subject of investigation or other unauthorized parties in a position where false or misleading information can be inserted into the investigative process to the detriment of the security agency. As a result, the scope and reliability of information available would be severely affected. The subject of investigation or other unauthorized parties, would be in a position to take countermeasures against continuing or future investigations.

The name of one Service employee, who is listed as the point of contact for the above two CIRs, was contained in the documents DELISLE attempted to breach. The reports contain the employee's name, position held at the time, and office telephone number. Additionally, DELISLE stated in his interview of January 13, 2012 that he breached information on a monthly basis since 2007. As such, any CSIS report to which DELISLE had access dating back to at least that time, has the potential to have been passed by DELISLE to the Russians. Therefore, any Service employee name / contact details on any of these previous documents also has the potential to have been passed. Further, as a ND officer in contact with the CSIS Atlantic Region office, DELISLE met at least one CSIS employee; he may also have met other CSIS employees during his previous postings in other locations. The Service is unaware, at this time, if and how many other CSIS employee names were potentially passed to the Russians. Their association to the Service may put these employees at risk by hostile intelligence services and terrorist groups.

The Service does not normally disclose information that would identify or tend to identify employees of the Service except in limited circumstances. Section 18 of the *CSIS Act* prohibits the disclosure of the identity of Service employees who are engaged in covert activities. Although not all Service employees act in a covert capacity, the disclosure of their identity may prejudice their ability to do so in the future. Provision of the identities of Service employees could limit their continued usefulness to the Service and prejudice ongoing collection of information and intelligence. Recruiting new employees to work in a covert capacity would be affected if the Service is unable to protect their identities.

Additionally, given that DELISLE admitted to providing contact lists of intelligence-related individuals and to providing information from key foreign partners, he has put at risk the security of these individuals and the partnerships of Canada's closest allies.

The scope of CSIS information passed since 2007 likely consists of Service source reporting, as well as information stemming from allied intelligence partners. The Service assesses that the provision of CSIS reporting to the Russians, over a period of time, has a likelihood of allowing this foreign government to identify individuals or technical methods used in the covert collection of information. As a result, DELISLE put into jeopardy the identities of confidential sources of information and the means by which CSIS collects, assesses, reports and communicates information and intelligence.

The Service does not disclose information, except as per section 19 of the *CSIS Act* that would identify or tend to identify confidential human sources of information for the Service or the content of information provided by a human source which, if disclosed, could lead to the identification of a human source. Human sources are considered crucial to the operation of any security service or intelligence agency. These may be people who volunteer information which they have received or who cooperate with the security agency when asked to do so.

A breach that concerns the disclosure of source information would be a message to current and potential sources that the Service could not guarantee the anonymity upon which their safety depends. Covert sources and the general public would be much less willing to co-operate with the Service and assist it in its investigation.

CONCLUSION

The January 13, 2012 arrest has prevented further breaches by DELISLE. However, significant questions remain unanswered including: (a) the extent, authorized or unauthorized, of DELISLE's access to information since 2007, (b) if, in his previous positions within ND, he was able to exploit access to similar sensitive information pertaining to Service reporting, other GoC department reporting or the reporting of allied services and, (c) the nature and extent of classified information breached by him to the Russians prior to January, 2012.

DELISLE maintained a Top Secret clearance, had access to a wide variety of TS / classified reporting, including CSIS reporting, as well as possible contact with various GoC and allied government partners. At his most recent place of employment at TRINITY, it is known that DELISLE had access to a range of CSIS reporting, including current and archived CIRs, Intelligence Assessments, Intelligence Briefs and other studies. Based on the RCMP interview of DELISLE, he was aware of his clearance level,

that he went through the indoctrination process, and that he was not to disclose (information). DELISLE was not / not authorized by the Service to disseminate information to a foreign government and, in so doing, may have: 1- damaged the Service's relationships with its closest foreign partners, thus reducing its capacity to inform the GoC of threats; 2- affected the safety / security of Service sources and that of its closest foreign partners; 3- informed the Russians of the extent of the Service's investigations; and 4- compromised Service methodologies, including how it collects, assesses, reports and communicates information and intelligence.

Based on CSIS analysis and our current knowledge of the totality of the compromise, DELISLE's unauthorized disclosures to the Russians since 2007 has caused severe and irreparable damage to Canadian interests.

APPENDIX

CSIS CAVEAT:

This document is the property of the Canadian Security Intelligence Service and may constitute "special operational information" as defined in the Security of Information Act. It is loaned to your agency/department in confidence. The document must not be reclassified or disseminated, in whole or in part, without the consent of the originator.

Canadian departments, agencies or organizations: This document constitutes a record which may be subject to mandatory exemption under the Access to Information Act or the Privacy Act. The information or intelligence may also be protected by the provisions of the Canada Evidence Act. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

Foreign agencies or organizations: This document is loaned to your agency/department in confidence, for internal use only. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator. If you are subject to freedom of information or other laws which do not allow you to protect this information from disclosure, notify CSIS immediately and return the document.

CSIS INTELLIGENCE ASSESSMENT (IA):

CSIS Intelligence Assessments are strategic assessments produced for the Government of Canada. These papers are relatively short, running from two to ten pages, depending on the issue and run the gamut of narrowly focussed analyses to broad threat-related trends. To ensure broadest dissemination to consumers with a need to know, they are produced at the lowest classification level possible but may be issued in multiple versions for different clients.

CSIS INTELLIGENCE REPORT (CIR):

CIRs provide timely tactical intelligence reports on specific issues in support of day-to-day government operations and policy requirements. CIRs are raw intelligence reports which are generally from a single source of reporting and from a single session of collection. CIRs may contain limited assessment in the form of a CSIS Comment.

Written Statement – 16 February 2012

BRIGADIER-GENERAL R.S. WILLIAMS, OMM, MSM, CD

1. Canada has serious national security interests in protecting information about intelligence sources and methods, including whether or not we possess particular capabilities, and even particular intelligence information. As indicated in our security classification definitions of injury, compromise of material classified at the Top Secret level would cause exceptionally grave injury to national interest.

Definitions – Injury Level to the National Interest	**Appropriate Classification**
Compromise would **not cause injury to the national interest**	**UNCLASSIFIED**
Compromise would cause **injury to the national interest**	**CONFIDENTIAL**
Compromise would **cause serious injury to the national interest**	**SECRET**
Compromise would **cause exceptionally grave injury to the national interest**	**TOP SECRET**

2. Disclosure of such information may reveal not only the content of the particular information, but the extent and nature of Canada's and allied capabilities, and where and how they may be directed. Our ability to protect our sources and our methods is fundamental to their effectiveness. By revealing certain products to a foreign entity, we reveal the very existence, scope, and the use of our sources and methods. When the type of information that the accused passed on is released, it compromises not just the information or intelligence that is gathered, but more importantly the source or method itself. This type of information is among the most highly protected of national security assets, by any government standard and goes to the heart of Canada's sovereignty and security.

3. The release of this information by the accused puts Canada's relationships with our partners in jeopardy. The inability to provide the assurance to our allies that we can and are safeguarding their intelligence could in extremis result in termination of access. Canada's closest intelligence allies are the United States, Britain, Australia, New Zealand and NATO. Given the shared border, we also have an additional close cooperation and mutual interest with the United States on various issues, and this incident has put that relationship at risk.

4. Working to build relationships and working with allies in support of mutual defence and security issues, is all part of the mission of the Chief of Defence Intelligence. These relationships assist us with providing credible, reliable and sustained intelligence to DND and the CF in support of decision making and military operations, and also in support of other government departments in the defence and security of Canada. As such, we share vital information with our partners that assist us in protecting the national security of our country, and protecting the security of our troops in various missions abroad. When we receive information from our allies it is incumbent on us to protect and safeguard that information. This compromise could put Canadians, CF members and allies in the field at risk.

5. This disclosure may also negatively affect our ability to receive timely and essential intelligence and information from our allies, which in turn puts the safety of Canadian citizens and of our Canadian Forces members in jeopardy.

Brigadier-General
Rob. S. Williams

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

P.O. Box 9703
Terminal
Ottawa, Canada
K1G 3Z4

C.P. 9703
Terminus
Ottawa, Canada
K1G 3Z4

UNCLASSIFIED

Your file Votre référence

Our file Notre référence
CERRID #916892

28 February 2012

Chief Superintendent Larry Tremblay
Director General National Security Criminal Operations
Royal Canadian Mounted Police
1200 Vanier Parkway
Ottawa, ON
K1A 0R2

Dear Chief Superintendent Tremblay,

This letter is in response to previous discussions between the RCMP's A/Commissioner G. Michaud and CSEC's DCSIGINT, Ms. S. Bruce, regarding a releasable (Unclassified) damage statement related to your Project Stoïque.

Based on CSEC's analysis of the material in question, that from 11 January 2012, the following statement can be made: "Should a non-allied foreign government have acquired the reports uploaded on 11 January 2012, it would have gained insight into matters of national security well beyond the intended intelligence purposes of the reports themselves. CSEC's preliminary assessment is that the damage caused by the release of these reports is high. The reports in question were all classified TOP SECRET, with special handling caveats to restrict their distribution to those properly indoctrinated within the Canadian government, the Canadian Forces, and close allied nations. Analysis of the contents of the reports could reasonably lead a foreign intelligence agency to draw a number of significant conclusions about allied and Canadian intelligence targets, techniques, methods and capabilities. Countermeasures taken as a result of insight (real or perceived) into intelligence capabilities could be costly in terms of lost sources and additional work to re-establish – where possible – these intelligence capabilities."

Should you have any questions concerning this statement, please contact the undersigned.

Sincerely,

James (Bud) Abbott
Director General SIGINT Programs
Communications Security Establishment Canada

Canada

Royal Canadian Mounted Police / Gendarmerie royale du Canada

OPÉRATION / CASE:	2011-3421		
I.D. LIGNE / LINE I.D.:			
SESSION NO.:	INAPPLICABLE		
DATE:	2012-01-14	HEURE / TIME:	18:41:34
SORTANT: O/G:	INAPPLICABLE	ENTRANT: I/C:	INAPPLICABLE
INTERLOCUTEURS:	SAMUEL MIKHAIL / [redacted]		
INTERLOCUTORS:			
LÉGENDE / CAPTION:	SM / JF		
LIEU DE LA COMMUNICATION: PLACE OF COMMUNICATION:	MILITARY INSTALLATION, ROOM 276, HALIFAX, NOVA SCOTIA		
AUTRE LIEU: OTHER PLACE:	INAPPLICABLE		
LANGUE(S) PARLÉE(S): LANGUAGE(S) SPOKEN:	ENGLISH		

SM: Hello, hum... my name is constable Samuel Mikhail. M... I... K... H... A... I... L. My regimental number is 48409, investigator with the RCMP, national security in Montreal, C Division. Uh... today I will be taking a statement with uh... [redacted] Military uh... identification number Foxtrot [redacted] is the Trinity Intelligence Head of Department. We are currently at Military Installation in Halifax. The room 276 uh... just uh, Mis... [redacted] and myself only present in room 276. Uh... the statement is in regards to police file number RCMP secure Pros 2011-3421. Hum... [redacted] uh... First of all, can you tell me a little bit about uh... uh... your duties and what do you do... basically.

JF: My duties... I'm the senior intelligence officer...

SM: Oh, excuse me, sorry I'm gonna... I'm gonna cut you off...

JF: _____.

SM: I'm sorry. Uh... for the date and time. Uh, right now we're gonna start the statement. Saturday evening, January 14th 2012. Uh... it's 6:43pm. Sorry about that.

JF: No, no problem at all. Hum... I'm the senior intelligence officer on the coast uh, _____ for the navy. I'm Trinity's intelligence for the department. I basically have the responsibility to manage an all source intelligence team which includes uh... about approximately, I believe [redacted] Uh... non-commissioned members. I have uh... uh, I have SIG... SIG... and support element detachment a Geomat (PH) detachment. And uh... uh... associated support. My role is basically to oversee uh, _____ navy support and as Trinity as the uh... basically the uh... Center for navy support for all intelligence for Canada.

SM: O.K. Can you tell me a little bit about your employee uh... Jeffrey Delisle.

JF: Jeffrey Delisle uh... joined me, or joined Trinity I believe around August of 2011. He laterally transferred over from uh... land forces, Atlantic area G2 staff where he's employed for uh... I'm not sure the period... _____ department there.

SM: So when did he join?

JF: Uh... he joined my staff in August of 2011. Uh... his actual employment, he came from the reserves was an intel-ops... intelligence operator and a non-

commissioned member. Took his commission and when he took his commission he was selected for navy and his transfer uh... land forces to Atlantic area which is the army to Trinity, he wanted to stay local so uh... the G2 there, [redacted] uh... contacted me and asked if I would be amicable of uh... uh... taking a lateral transfer of Sub-Lieutenant Delisle to my organization. I uh informed I had no objection as he was an Int-op and I knew he would had previous experience and, and so uh... he uh... joined my outfit in August of 11. Uh... he's uh... Again, he came from the ranks so he had a good deal of experiences in Int-Op that was evident when he was uh... as a Sub-Lieutenant he wasn't what you normally expect a Sub-Lieutenant to be. He was well... well versed in his trade craft. He uh... I didn't have any issues with him, with his uh, work. Uh... he was always on time. He never... I've never seen him panic when he has his tight deadlines. He met his deadlines uh... the work was accurate and, and uh... in time-line uh... there was uh... no uh... personal issues I can note such as uh... alcoholism or drugs. He... came to work, did his job, met his deadlines and, and... didn't fly in my radar because of that uh... He was... basically uh, doing what was expected, especially as a Sub-Lieutenant in a very busy job as a threat assessment analyst.

SM: O.K. And uh... so, you, you... you're Mister Delisle's immediate supervisor, correct?

JF: I am. Well, yes, uh... by... largely because of proximity, yes because uh... and at the end, [redacted] Hum... people who working down here in this building fall directly under my supervision because I have the greatest chance to observe them.

SM: O.K.

JF: Normally it would be a Lieutenant looking at them but... they're just, [redacted]. because of the proximity I was the one who would... who would take the majority of the notes on Sub-Lieutenant Delisle.

SM: O.K. And what's his rank?

JF: Sub... Sub-Lieutenant. Uh... it is army term, it's the Lieutenant. It's basically a... a bar and a half uh... one... The next promotion is Lieutenant which is basically, the rank when we expect the officers to be fully versed in their... in their craft and uh... fully capable. As a Sub-Lieutenant you're given more free chances, I guess for better words to screw up uh... But uh...

SM: What, what, was uh... if he was going on... staying on the same course, he would have obtained his Lieutenant when?

JF: Uh... it's 4 years... or 3 years. So he would have been probably due Lieutenant uh... I assume it's 11 of next year or... not this year.

SM: Yeah...

JF: And, and for Lieutenant, it's just... it's basically it's time-in. It's not uh... it's... _____ are not like _____ promotion unless you screw up. Like you can... you got alcohol abuse or you've been _____ warning (PH) a charge. The CO is basically gonna... is given the discretion to say yes or no to a promotion and for Lieutenant it's basically your time-in with honorable service and uh... and good conduct. And, and basically doing your job efficiently otherwise, you're basically given, you do your time and you're getting your promotion. Hum... Yeah.... with, with uh... No... with Delisle, I mean uh, the issues with him were, were, were a lot of health related as I could see. I had a chat with him uh... about that because I explained to him that when he was... he was talking about his uh... insulin issues, diabetics and uh... he was in a... I believe in a _____category, which means he, he wouldn't be employable at sea. I informed him that... uh, the optics are... and, and the reality is if he couldn't sail, his chances or... of being retained as a navy intelligence officer would be, would be basically uh... nil.

SM: Hmm.

JF: Uh... because if you can't be employed in the element you're, you're told to be in... then uh... you can't be em... employed.

SM: Uh-hum.

JF: Pretty cut and dry. So I know he had that on his... on his plate so obviously where he's... likely, he was... he was going to get the check ups and... _____.

SM: (Coughs.)

JF: And uh... I... he, he kept me updated, he said they switched medication the last I'd heard and he... they were waiting 30 days to see how that played out. But uh... I didn't get the feeling that this something that he was, he was... _____ promising for him. Prior to that, he had issues _____ with his shoulder. Couldn't do his uh... express test, which is another requirement for uh... well it's the requirement for the promotion even to Lieutenant but also too... it's uh... one of these things that he uh... the command and, and... the CF looks to make sure you meet your standards. Physical fitness if a huge one for the military, obviously and uh... his physical standards were obviously suffering because of either medical issues or uh... (tsk) or medical issues _____ shoulder and he's diabetic. So uh... I, I guess _____ from that point of view is... probably his outlook wasn't uh... positive to his, his uh, retainment if he, if he couldn't get that in order because the... the Forces is now in the, the position where... and it's widely been broadcast that _____ major has gone through and told his message to folks... If you basically don't pass your express to us or you don't meet the core requirements, the Forces will look to release folks now. They're not gonna retain folks to uh... uh... because in the past, they were short on bodies and they needed these people so they sort of give waivers or extensions. Now that we're at uh... extra strength uh... the force is getting selective and they're actually... not _____ not offering up to even folks who make those requirement uh... if they're just like coasting by.

SM: O.K.

JF: It's, so... uh... that was my concern with Delisle. I could see that he was gonna be an issue with medical and not being able to see it fail and uh... then not be able to do the PT test on top. That was my concern with him. It wasn't uh, it wasn't financial or any other issues I could note. My big concern was I, I was... thinking that the medical thing was going to do him in.

SM: O.K. Hum... What uh... databases does uh, Sub Lieutenant Delisle have access to? In, in the course of his duties?

JF: Right. Uh... It was uh... as a threat assessment officer for Trinity. His duties required him to uh... go all source. Grab all the sources he could to look for uh.... access pertaining to terrorism, cyber crime, espionage hum... civil threats, uh... health threats, so that, that took him across the whole gamut from the unclass realm for health iss... health threats to public service sites or, open to public for sites for health issues, right through to the highest system that we have uh... Spartan, which is our top secret Canadian Eyes-only system. And on those systems, in particular Spartan, uh, he had robust access to all source intelligence from all our partners, especially the Four I's community which is Australia, Canada, Great Britain and the United States. And that includes its [redacted] uh... [redacted] intelligence such as [redacted] uh... straight through to Canada's only reporting, such as CSIS reports or hum... Privy Counsel Office reports because we have a tunnel into what, what's called Mandrake, which is the other gov... Canadian other government department's top secret uh... Canadian Eye's only system. RCMP's on that... CBSA, TC, the... basically, the... the, the big partners and he would have full access to that. On [redacted] Hum... the only thing I'm not sure if he is... if he had access to [redacted] which I will inquire and uh report back. If he had a [redacted] .. [redacted] account, that would give him, a... access to further hum... broad report, that [redacted] hum... which would further increase the issue of uh... basically with that, _____ [redacted] you basically have everything and uh... but uh, if I was to give a ratio or percentage of what, the general intelligence he could

have accessed, it's in the [redacted] or closer probably [redacted] because of the nature of his job and the access he had.

SM: So he produced and the... the threat assessments for the Navy?

JF: [redacted] and the nature of that job requires them to work long hours and extended hours and uh... off on the weekends as well, which is nat... natural for the course. So, any... after hours work or any weekend work is normal and uh... would not uh, flag anything [redacted] _____ just have to come in and do these things. So uh... working odd hours and working weekends would not be an anomaly for the job. In fact, it would be what's considered to be normal for that job.

SM: O.K. So, according to, lo... to what you know about his schedule uh, Mister Delisle's schedule...

JF: Uh-hum.

SM: He... is very normal and is very routine that he would worked evenings and weekends, here and have access to all those databases you mentioned.

JF: Yes, I... I mean normally that, your day is still 8:00 to 4:00, but uh... when the crunch time's coming up uh... you, you would be _____, so I would say it's not every weekend but maybe once a month, it's... there'd be a requirement but the fact that he was doing that, it would be not _____.

SM: _____, other than this location here uh at uh Trinity uh, uh... does he have an office anywhere else or does he work somewhere else?

JF: No, his office is down here but uh... the fact that he's...

SM: Can you... you describe what room or what office uh...

JF: [redacted] He was the only individual using those systems and uh... [redacted] Uh... so but Delisle's space was dedicated to him. That was only for his to use and uh... uh... [redacted]

SM: O.K. So what's his uh security and the nature of his classification?

JF: Well he has the top secret special intelligence uh... access. Again...

SM: What is that exactly?

JF: Yeah, it means that uh... that he has access to [redacted] report, [redacted] uh... it's usually also the realm of uh... [redacted]

SM: Yeah but how... in, in comparison to the other levels, what does that like in the hierarchy? 'Cause I don't, no...

JF: It's, it's... it's above top secret. The... they have... you have secret, you, you have unclass, confidential, secret, top secret and then top secret special requirements. He didn't have every requirement that we have uh, hum... but he had sufficient quantities to give him the bulk of the... what was there.

SM: Yeah. So, in his office uh, when... there's work stations from which, you know, no other person went there, back there in his cubicle to use his computers?

JF: No...

SM: O.K.

JF: No, and like uh... I, I made that as a... as a default rule, which I enforced in that space but uh... his... Even when he was out of office, that we wouldn't use his

spaces. And uh... his machines would be left untouched.

SM: Perfect. What agencies uh... whether foreign or domestic or countries uh... uh... provide, provide, provide information to this unit, to... W... what other countries basically or partners share their information with, with Trinity?

JF: _____.

SM: For you, for your databases?

JF: Right. The primary 'cause, the primary uh... partners are the United States obviously and Great Britain. The United States is probably the, the, the bulk of our engagement. Uh... that's probably in the [redacted] The United Kingdom [redacted] uh... in [redacted] is uh... _____. It's something that I took on as a project to try to [redacted] and especially their [redacted] knows as [redacted] which is basically _____ Trinity, so we had a commonality... So uh... I, I was very forward leaning with my folks to say, press engagement, to reach out to _____ and to uh... collaborate as much as I could. And if I had told my folks to make sure they uh... that's all the systems that they could, they could get into leverages _____ because the... I didn't want them to s... just to stagnate and... and not engage so I, I, I told my folks. I said, "I want you to engage, you're our partners and uh collaborate." Because uh... and in the intelligence world, _____ for Canada. We're uh... we're... we don't provide near what we receive so I'm always keen to make sure that we re... return not just take _____.

SM: Uh-hum.

JF: So uh... I mean there's a very _____ States it's probably... [redacted] So, anything we provide uh... it's uh... it's, it's key, so I push my folks to, to, to do that.

SM: So, any other countries? Uh... s... s...

JF: Australia as well but uh... [redacted] Uh... but also there's uh...NATO, uh... to a smaller degree just because the bulk of our intelligence is either uh... we _____ Four I's or Two I's so it's been... lent itself to working _____ tightly or closely. Hum... our primary n... uh.. [redacted] and that's where we had the greatest relationship. We actually have a [redacted] So I had, I have extremely good connections there and I leverage them quite well.

JF: Uh, for the [redacted] _____. And uh, those really... and... and also on the [redacted] And the [redacted] _____ and uh, again, we have had an [redacted] with them as well, and uh, we've been increasing our... our coverage in there as well.

SM: O.K. Uh, you know the... the nature of the investigation,

JF: Yes.

SM: Of the RCMP.

JF: Yes. Yes.

SM: Uh, the.. the investigation on Mister Delisle.

JF: Yeah.

SM: Um, do you know if... if anyone else in... in this office would be associated to Mister Delisle's activities in this investigation...

JF: _____...

SM: Or would be collaborating with him?

JF: No, I mean, I didn't even find out... That he was uh... supposedly doing this, uh, shocked me. I mean, uh, this is not what I expected to... to hear even from him, of him. Uh, so... like you said, I... I looked for issues obviously from the personnel side because that impacts their work. Uh, there's always been issues with folks either it's like they're just stressed out at home but uh, I... I've never seen any... any signs like this that would lead me to think that he was uh, subversive or uh... or seeking out capital gain. I'd... I'd never suspect... for Delisle, there's no way. Like, flags for finance? _____ which I, which I... I

learned previously though, was the issue that flagged me was when he went on his trip to Rio... Rio de Janeiro and he went by himself. That... to me, it wasn't a financial _____ that, when that was a character check. _____ when he went over by himself when I knew he had a girlfriend. My thought was obviously he was going there to socialize with the female gender. Uh... and then, but... _____ that was what I found on that trip but then in a fairly short turnaround, he then went to Cuba. And that sort of... that was when I wondered: "Wow, O.K. how's he affording this?". So that, that did cause a financial flag, but I didn't see anything, I didn't see these issues like, Bell Company is calling us saying you know, Delisle's account's past due. Uh... 'cause that's a flag we have to act on. We can't... we can't punish a person for taking trips.

SM: Of course.

JF: Uh... Until we actually get those... those uh... warnings from either a credit company or a NCIU, uh... we're... we're tied. We can show concern, we can show interest but we can't... we can't take action for someone taking trips.

SM: Has he ever spoken about his... his trips to Cuba or Brazil to you or to anyone else here?

JF: Yeah, when he got back I was...

SM: And so, what... what... what has he said about those trips?

JF: Yeah, when he got back from Brazil, obviously, I was anxious to see what uh... how the trip went, just because it was kind of a surprise that he'd picked Brazil. And he mentioned to me that he didn't have a good time down there and I found that kind of strange that uh, but uh, it didn't.... I guess, meet his expectations was what seem to come from him. Uh, he... he basically said it wasn't a good place to go by yourself. Uh, he just uh... it didn't hit what he expected, I guess. Uh, so he... he... he wasn't pleased with this trip is what I get from uh... _____ I didn't... I didn't pry any deeper because it wasn't my... my uh, privy to say, you know, "Why wasn't it good?" Uh... the Cuba, he didn't mention anything about Cuba. He just uh... it was just... it was just... he never went to Cuba. He never told me about it and I never asked.

SM: O.K.

JF: Uh so, for each one he just:.. he knew the regulations of _____ NCIU and uh, as far as I know, he went down and talked to NCIU and uh, informed them that he was going to... to Cuba in particular and uh, I don't feel _____ either.

SM: O.K,. Do you know of any other trips he's... he's made?

JF: No, uh... Obviously Rio and Cuba, those flagged 'cause they're out CAN (PH) and uh, you have to see it, you have to note that to your... to your chain.

SM: O.K. So you don't think that anyone else did the same thing that he's done in terms of this investigation?

JF: No. No. No, definitely none of my other folks have gone to... to uh... uh, Brazil. I mean Cuba's a... that's a common destination for Canadians but uh... uh... No, I haven't seen any signs of shadow from other folks.

SM: Do you know any reasons why Mister Delisle would do, uh, what he's alleged to be doing or what he's alleged to have done?

JF: Well I mean, when he... it's always the hindsight 20/20 but what I mean when the... when the alleged acts happened, I started to think O.K. What... what signs might I have missed or what signs could I have misinterpret... misinterpreted. For me, obviously his medical. Uh... I think that, that would give him a... that could give him a financial incentive because uh, he also mentioned to me that uh... which I thought... I thought was surprising about a week ago or so, was that he wasn't going to re-app (PH) when his uh, when his terms... his... his... his mandatory terms of service had ex... expired. Uh, it... I... I... I just found it strange that the person was saying that uh... that would say that. "I don't think I'm gonna... I'm not gonna _____."

SM: When did he say that?

JF: About a week or so ago. It was just out of the blue. It's just... we were talking and he said... I forget how... how we got to the topic but he just said: "Well um, when my mandatory period... period of service expires,"... which he had to do 'cause they sent him back to school for a degree, he was gonna... he wasn't gonna... he was just gonna stop. My first thought in my head was well, it's not

gonna matter anyways, you're gonna fail because of medical issues. So... it... it wasn't just a... a... bravo statement because... To me, I... I... I see his medical statement being his downfall. Uh.

SM: Hum.

JF: The bump shoulder uh, the... the diabetes. To me it was just time, he's gone.

SM: O.K. Um, so he's been at Trinity since August 2011.

JF: Hum-hum.

SM: Uh,.. so it's possible that since August 2011 he's been allegedly... he did... you know doing the uh...the accusation?

JF: Yes.

SM: Uh, is it possible that even before he joined Trinity in the summer of 2011 that he... he's been doing... he's been doing this stuff for a while?

JF: Yeah, it's possible, yes, because he had access. Uh...

SM: And was he TSSI before August...

JF: Yes...

SM: 2011?...

JF: Yes... Uh, like I said, he was an intelligence operator before,

SM: O.K....

JF: Which gave him that access.

SM: So since... since what year would you would say he's TSSI?

JF: Um...

SM: Approximately.

JF: For me, it's 5 years. I would... I would estimate. I mean I don't have his file in front of me but uh, as an Int-Op, you're... you're... you're given TSSI.

SM: O.K.

JF: You need it... you need it for your job.

SM: O.K. Is it the highest level of classification in the mil... in the Military or the Navy?

JF: It is... it is, in the Military, there's TSSI is... is the highest uh, generally like basic caveats, you can get to. There's always uh... programs he can get right into.

SM: O.K.

JF: Uh, we've got a couple out here that uh... I know... I know he wasn't right into, right into those but he... but he... the access he had was extremely substantial.

SM: O.K. The potential or possible consequences to him sharing information with...

JF: Astronomical.

SM: People? Uh, let's say from the... the... the... the least, the least serious to what is the most serious... damaging ...

JF: The least...

SM: Consequences.

JF: The least serious is uh... what we call a classified a _____. It's more like just keeping it out of the public domain for government use. That would just be like: "Oh don't do that again please." from your partners... to uh, the Top Secret special information that... which would cause serious, grave... depending on the... the... manner of release and who it went to.

SM: Yeah.

JF: Uh, that's very different, who it went to.

SM: Yeah.

JF: [redacted] Yes, it _____ clear people in that community but stays in that community. If he is _____, if, as alleged, if he has released information to say, the Russian Intelligence Service, that will cause a... that... a... I... I... I'm just like... I can phantom the response the globe will be facing. Hum...

SM: What, what would be the most serious consequence?

JF: It'll stop. We'll lose our intelligence and for instance, we have a ship over in... in the... the Mediterranean [redacted] that information and those... that [redacted] could... could lead to death of our sailors, in... in the worst case scenario.

SM: If, from what you're saying in the worst case scenario, people's lives could be seriously in danger?

JF: Oh definitely, yeah. If he passed information about what the [redacted] reporting was doing, he could expose or provide information to the... to the...

SM: Whoever.

JF: To whoever. And that uh... that puts... puts their... either their operations or their... even their lives in jeopardy.

SM: So we're talking about military members' lives at risk?

JF: Also civilian members uh... government members. CSIS, he has access to CSIS reporting. Uh, for instance uh, they were in places in the Middle East and uh, we were receiving that information because we have a ship over in that area, the fact that he could disclose that, to other nations, could a) embarrass... the... our government and cause political ramifications on our government and also close intelligence sharing between organizations because of lack of trust.

SM: O.K. I'm more concerned about uh... like, people's lives.

JF: _____ definitely, I mean, people, people who could... who could

SM: Like seriously be hurt, you said military members, potentially uh, CSIS agents?

JF: Yes. I mean uh...

SM: And civilians as well in different countries or one specific country or what?

JF: Yeah, I mean, if you really say... retur (PH), uh, a sensitive eyes only Canadian product to uh, another nation and it's critical in that nation, uh, we've seen it in places like Iran where they... they went against the British Embassy because of open source issues or just perceived issues, to release uh... I mean there were also this Wikileaks issue. The release of the Wikileaks documents setback the US and endangered a lot of their operatives. I mean, depending on what was in that information, if it... they don't... they wouldn't name an individual, you know, in the information. That's... that's a safety issue where they... they just won't do it. But, uh... not having information is just as dangerous as giving it out. Because if we lose that information from our allies, we might not get that indication of an impending terrorist attack, for instance. The worst case scenario.

SM: O.K....

JF: And then our ships could get uh, exposed to _____... (noise) serious and grave or vicious...

SM: Hum, is it possible for the Military to know the information they know now about Mister Delisle? Is it possible to backtrack and find out exactly what he _____ what information he has shared with other people he's not suppose to or what information he's taken out of this office?

JF: Obviously, we're gonna try that because that's critical that we do that because we're gonna be in damage control with our partners. Uh, the tactical thing is what I need to investigate with you or N-6 which are our... our... IT folks. To find out who can get things like... the M-3 Search Engine. [redacted]

SM: O.K.

JF: So, that's... that's... But we will be doing this, to find out.

SM: O.K. Hum... Is there anything else you'd like to add Sir, to your statement?

JF: Other than that I was...I'm... I was shocked. Uh, uh... I'm... I'm extremely concerned about how this is going to affect my relationship with my partners, uh, because I was... I was taking large strive in our engagement, and I think this is going to push us back to the stone age. If it gets to the worst case scenario and uh, this is uh, it's... it's unphantomable. I mean...

SM: Tell me how do you feel right now?

JF: Well, betrayed... uh... uh... sort of... it... it's almost like in denial. It's... it's... just... it's... I can't phantom... uh... the alleged charge of espionage by one of my folks. Uh,... uh.... it's _____ obviously too, because uh, this could... destroy everything

I've done here, _____. It's not a good feeling again and obviously being the direct supervisor. Also the... the concern I guess is how this will look on me, because in the end, I can say it, I was responsible for him. So, uh, yeah, I might not have been... been able to stop him directly but still I'm... I' m still his direct supervisor, so... Yeah, I don't... I don't see this being an issue I can just say: 'O.K., it wasn't me." _____ what's gonna happen to myself, to be honest.

SM: O.K. Is there anything else you would like to add?

JF: Other than I hope that we find out what happens, good or bad because uh, this is uh, this is above the individual, this is... this is... a key to everything we do here in Canada. Uh, this is uh... _____, I... I... I tell you it's uh... if he's guilty, I hope he goes to jail for... for life, and if he's innocent, well, he's innocent but uh, uh... I have no pity if he did do it, and uh... I... I... would like to see him get the maximum sentence if he did do it because there's no excuse. And uh, I have... I have no... no compassion for... for traitors.

SM: O.K. Is there anything else you would like to add?

JF: No other... other than that... I... I thank you guys for your... your... your aid in going through this and uh... yeah, anything we could do, anything I can do, I will uh... I will... assist as well as I can.

SM: O.K. Any, any, any other, any other things you would like to share or... or?

JF: No, just like I said, I would like to see this resolved as... as quickly as we can, just so because uh...answers need to be found soon.

SM: Do you have any questions for me?

JF: Other than just how we... are we gonna be apprised about how things progress uh, because we're... we're... we're gonna be in a situation where... what if the allies find out. What's our... what's our... storyline. What's our...

SM: I'm sure at this point uh, there's a lot of people talking over here

JF: Yeah...

SM: and I'm sure... I'm sure your department and your commander will... will be updated at some point. Uh, but as for me, I uh, I uh, I uh, personally...

JF: Right...

SM: Can't answer those questions right now...

JF: Right, I know...

SM: _____...

JF: _____...

SM: O.K.

JF: So, that's my biggest concern is uh... what... what's gonna happen and what do we do?

SM: O.K.

JF: It's... _____ ... _____. It feels like... it's like a limbo for me.

SM: O.K.

JF: It's uh, I don't know what's gonna happen with this... this individual, I don't know where we're at, I don't know what our allies know.

SM: O.K.

JF: And so...

SM: O.K. So this concludes the statement. It's currently 19:17. Thank you very much, [redacted]

JF: Thank you.

FIN DE LA COMMUNICATION